Математическая модель гибридной системы противодействия угрозам нарушения информационной безопасности в информационных системах на основе квантового распределения ключей и постквантовой криптографии

Д.А. Кулаков, К.З. Билятдинов

***Аннотация* — Представлена математическая модель гибридной системы обеспечения информационной безопасности в информационных системах, основанная на комбинированном использовании квантового распределения ключей и постквантовой криптографии.**

Модель предназначена для минимизации вероятности компрометации каналов связи и поддержания непрерывности функционирования при ограниченных ресурсах. Разработаны допущения, ограничения, структура модели и описаны компоненты модели. Доказано, что гибридный подход позволяет обеспечить требуемый уровень защищённости в информационных системах, включающих территориально распределённые элементы.

***Ключевые слова* — квантовое распределение ключей, постквантовая криптография, информационные системы, информационная безопасность, гибридная модель, инфраструктура.**

I. Введение

Современные информационные системы (далее – ИС) характеризуются высокой сложностью сетевой топологии, разнообразием узлов связи (как элементов ИС) и высокой скоростью передаваемых и обрабатываемых данных. Особенно это характерно для ИС в промышленных и транспортных инфраструктурах — таких как промышленные предприятия с автоматизацией технологических процессов производства, сети управления движением поездов, энергетические диспетчерские комплексы и системы логистики на железнодорожном транспорте.

В настоящее время имеющиеся направления и перспективы дальнейшего развития квантовых технологий представляют угрозу для традиционных криптографических алгоритмов (RSA, ECC, DH) [1, 2, 3, 5]. Адекватное противодействие существующим угрозам информационной безопасности ИС требует разработки и внедрения новых моделей защиты ИС, устойчивых к различным деструктивным воздействиям (атакам) с применением квантовых технологий. Одним из рациональных технологических решений этой актуальной задачи является гибридизация квантовых и постквантовых методов, объединяющая физически защищённое распределение ключей шифрования (QKD) [2, 3] и математически стойкие алгоритмы на основе решёток и кодов (PQC) [1, 6].

Для практической реализации предлагаемого технологического решения целесообразно формализовать процессы генерации, распределения и ротации ключей шифрования в гибридной архитектуре безопасности для распределённых ИС, а также для минимизации риска компрометации ключей при эксплуатации ИС в реальных условиях [4, 7].

Таким образом, постановка научной задачи исследования будет заключаться в разработке математической модели гибридной системы противодействия угрозам нарушения информационной безопасности в распределённых ИС на основе рациональной интеграции QKD и PQC (далее – Модель).

Для разработки предлагаемой Модели необходимо:

1. Формализовать процессы взаимодействия между квантовыми и постквантовыми подсистемами защиты [1].
2. Определить критерии эффективности: вероятность компрометации (P_{comp}), время обновления ключа (T_{upd}), скорость безопасного трафика (R_{sec}).
3. Построить алгоритмическую структуру модели, описывающую преобразование входных данных (параметров каналов, уровня угроз) в выходные (оценку устойчивости, выбор механизма защиты).
4. Определить допущения и ограничения применимости модели в промышленных и транспортных ИС [4].

II. Основная часть. Допущения и ограничения

Назначение Модели:

1. Оценка защищённости ИС при наличии гибридной криптографической инфраструктуры.
2. Оптимизация распределения ключей шифрования между подсистемами QKD и PQC.

3. Формирование решений по выбору стратегии защиты в зависимости от состояния каналов связи и уровня угроз информационной безопасности.

Модель обеспечивает адаптацию ИС к текущим условиям эксплуатации, включая ограничение длины оптических каналов связи, вариативность трафика и наличие внешних воздействий.

Допущения:

1. Узлы сети связи синхронизированы и связаны через сертифицированные оптоволоконные каналы.
2. Подсистема QKD реализует протокол BB84 или MDI-QKD.
3. Подсистема PQC использует утверждённые NIST алгоритмы шифрования (например, Kyber, Dilithium).
4. Все ключи шифрования хранятся и обрабатываются в защищённых аппаратных модулях (HSM).
5. Вероятности компрометации каналов связи статистически независимы.

В базовой конфигурации модели вероятность деградации квантового канала и вероятность криптографической компрометации рассматриваются как статистически независимые события. Данное предположение вводится как модельное допущение, направленное на упрощение аналитического описания системы и получение интерпретируемых оценок.

Указанное допущение корректно при отсутствии координированных межуровневых атак. В случае их наличия модель может быть расширена использованием условных вероятностей либо введением параметра корреляции. Таким образом, независимость рассматривается как рабочая гипотеза базовой версии модели и определяет границы её применимости.

Ограничения:

1. Модель не учитывает влияние квантовых ретрансляторов и спутниковых каналов.
2. Влияние шумов и затуханий оценивается по усреднённым значениям.
3. Не рассматривается компрометация внутренних HSM.
4. Атаки на физический уровень (side-channel) не моделируются в рамках предлагаемого технологического решения.

Теоретические основы разработки Модели.

Гибридная система включает три взаимосвязанных подсистемы:

1. Подсистема QKD — отвечает за генерацию и распространение симметричных ключей с информационно-теоретической стойкостью [2, 3, 8].
2. Подсистема PQC — выполняет аутентификацию и резервное шифрование классического канала, обеспечивая криптографическую стойкость при недоступности QKD [1, 6].
3. Подсистема управления ключами (KMS) — координирует ротацию ключей, их смешивание и распределение между узлами.

Математическое описание.

Пусть сеть включает множество узлов $V = \{v_1, v_2, \dots, v_n\}$.

Каждая пара узлов соединена классическим и квантовым каналами.

Для узла v_i вводятся параметры:

- $R_{QKD,i}$ — скорость генерации ключей QKD;
- $P_{fail,i}$ — вероятность отказа квантового канала;
- $P_{PQC,i}$ — вероятность успешной криптографической атаки на PQC-алгоритм;
- W_i — весовой коэффициент критичности канала.

Общая вероятность компрометации канала, формула (1):

$$P_{comp,i} = (1 - R_{QKD,i}/R_{th}) \cdot P_{PQC,i} + \gamma \cdot P_{fail,i} \quad (1)$$

где R_{th} — пороговая скорость QKD, γ — коэффициент влияния отказов на компрометацию.

Вероятность компрометации определяется формулой (1), используемой в рамках настоящего исследования как модельная интегральная оценка риска. Данное выражение не является строгим следствием теории вероятностей или криптографической теории стойкости, а представляет собой аналитическую инженерную аппроксимацию, предназначенную для агрегированного описания совокупного воздействия отказов и атак.

В рамках статьи полученные значения интерпретируются как модельные показатели, позволяющие сопоставлять различные режимы функционирования системы.

Скорость безопасного трафика, формула (2):

$$R_{sec} = \sum_{i=1}^{n} W_i \cdot R_{QKD,i} \cdot (1 - P_{comp,i}) \quad (2)$$

III. Структура модели

Модель представлена в виде последовательной схемы преобразования данных.

На Схеме 1 представлен функциональный контур модели, реализующий отображение:

$$\boldsymbol{\mathcal{F}}(\boldsymbol{\mathcal{K}}(\boldsymbol{\mathcal{C}}(\boldsymbol{\mathcal{N}}(\mathrm{S(t)})))) \rightarrow \{\mathrm{P_{comp}}, \mathrm{R_{sec}}, \mathrm{I_{res}}\} \quad (3)$$

где:

$\boldsymbol{\mathcal{N}}$: $\mathbb{R}^m \rightarrow \mathbb{R}^m$ — оператор предобработки и нормализации входных параметров;

$\boldsymbol{\mathcal{C}}$: $\mathbb{R}^m \rightarrow$ {QKD, PQC, Hybrid} — оператор выбора режима защиты на основе оценок состояния сети;

оператор гибридной генерации ключевого материала:

$$K_{hyb} = K_{QKD} \oplus K_{PQC} \quad (4)$$

Для количественной оценки устойчивости функционирования вводится нормированный индекс устойчивости

$$I_{res} = \frac{R_{sec}}{R_{max}} \cdot (1 - P_{avg}) \quad (5)$$

Показатель (5) является модельной метрикой, предназначенной для сравнительного анализа режимов функционирования распределённой информационной системы, использующийся как интегральный индикатор состояния инфраструктуры в рамках разработанной модели. Значения, близкие к единице, соответствуют устойчивому режиму функционирования, тогда как снижение индекса указывает на необходимость адаптации параметров защиты.

Применение операции (4) рассматривается как инженерная реализация гибридной криптографической схемы. Стойкость результирующего ключа обеспечивается при условии достаточной энтропии по меньшей мере одного из входных компонентов, их независимости и равенства длины.

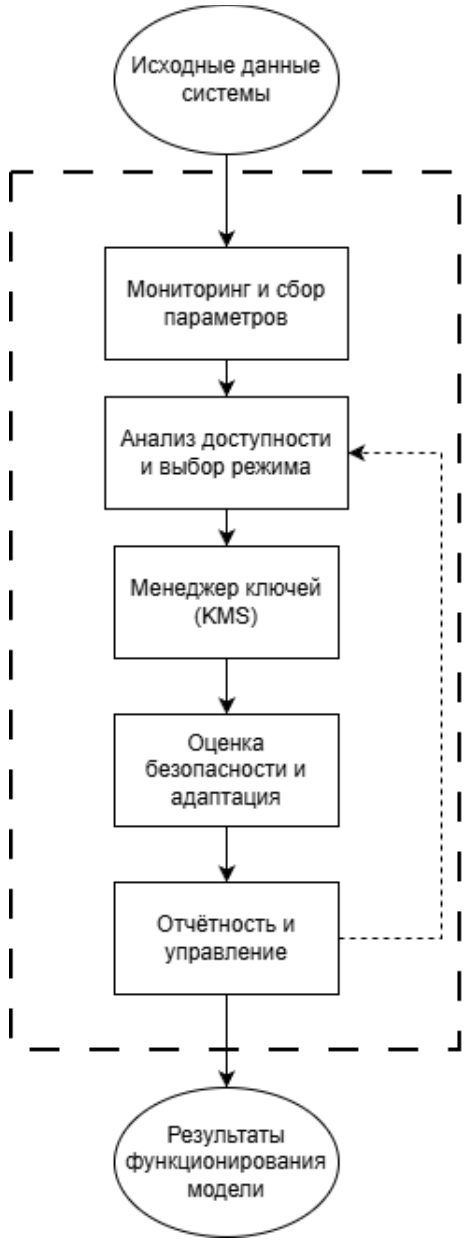

Рисунок 1 – Схема Модели

Соблюдение требований синхронизации и однократности использования ключевых блоков является обязательным условием корректности реализации.

оператор итоговой оценки устойчивости:

$\mathcal{F}$: $\{K_{hyb}, S(t)\} \rightarrow \{P_{comp}, R_{sec}, I_{res}\}$.

1. Блок входных данных (БВД).

1.1. В БВД определяются параметры ИС: RQKD, P_{fail}, P_{PQC}, W_i, уровень угроз, состояние каналов.

1.2. Формируется набор исходных параметров, поступающих в Модель. Эти данные отражают текущее состояние сети, используемые каналы, а также контекст угроз и критерии критичности узлов.

2. Блок мониторинга и сбора параметров (БМСП).

2.1. В БМСП осуществляется измерение, фильтрация и нормализация параметров, а также формируется вектор состояния S_i (t).

2.2. Преобразуются исходные данные в формализованные параметры для анализа: устраняются шумы, агрегируются измерения, создаётся вектор состояния канала.

3. Блок анализа и доступности выбора режима (БАДВР).

3.1. В БАДВР проводится проверка условий для QKD, PQC или гибридного режима.

3.2. Формируется матрица доступности M.

3.3. Вырабатывается решение о том какая подсистема (QKD/PQC) должна быть активна, исходя из реальных параметров сети.

4. Блок менеджмента ключей (БМК).

4.1. В БМК происходит генерация и смешивание ключей:

$K_{hyb}=K_{QKD} \oplus K_{PQC}$; ротация, распределение по критичности W_i.

4.2. Преобразуются криптографические ресурсы в гибридный ключ, обеспечивающий баланс физической и математической стойкости.

Таблица 1. Основные параметры модели

Параметр	Диапазон	Описание
R_{QKD}	0–100 кбит/с	Генерация квантовых ключей
P_{PQC}	10^{-8}–10^{-5}	Оценка криптостойкости
P_{fail}	0–0.1	Отказ оборудования или шум
R_{th}	50 кбит/с	Критическое значение перехода
P_{comp}	0–1	Интегральный риск
W_i	0–1	Важность канала или узла

5. Блок оценки безопасности и адаптации.

5.1. Расчёт показателей: P_{comp}, R_{sec}, I_{res}.

5.2. Проводится сравнение полученных значений с порогами, активация корректирующих действий.

5.3. Определяется устойчивость системы.

5.4. При необходимости проводится адаптация стратегии защиты.

6. Блок отчетности и управления (БОУ).

6.1. Формирование отчётов, передача в SIEM/АСУ, обратная связь.

6.2. БОУ передаёт результаты в управляющие системы, обеспечивает коррекцию параметров модели.

Выходные показатели: вероятность компрометации P_{comp}, скорость безопасного трафика R_{sec}; индекс устойчивости I_{res}; оптимальные параметры защиты.

IV. Анализ устойчивости модели и сценарии функционирования в распределённых ИС

Одним из ключевых требований к разрабатываемой Модели является обеспечение устойчивости функционирования распределённой информационной системы в условиях деградации отдельных подсистем защиты, а также при воздействии комбинированных угроз информационной безопасности. В отличие от статических криптографических решений, предлагаемый модельный подход ориентирован на адаптацию параметров защиты в зависимости от текущего состояния квантовых и классических каналов связи.

Устойчивость Модели в данном контексте определяется способностью системы сохранять заданный уровень защищённости при изменении входных параметров вектора состояния S(t), включая снижение скорости генерации квантовых ключей, рост вероятности отказов оборудования и увеличение криптографической нагрузки на подсистему PQC.

В рамках модели учитываются не только вероятностные отказы и деградация каналов связи, но и потенциальные активные воздействия на инфраструктуру системы управления ключами. Активный противник может инициировать атаки на классический канал передачи служебной информации, предпринимать попытки нарушения синхронизации квантового распределения ключей либо создавать перегрузку ключевой инфраструктуры. В модели подобные воздействия отражаются через динамическое изменение параметров вероятности отказа и вероятности криптографической компрометации во времени, что приводит к адаптивному переходу между режимами QKD-доминантного, гибридного и PQC-доминантного функционирования. Таким образом, модель позволяет учитывать изменяющийся характер угроз без выхода за рамки инженерного описания.

Для формализации анализа устойчивости вводится понятие сценария функционирования, под которым понимается совокупность условий эксплуатации ИС, определяемых набором параметров:

$$\Omega = \{R_{QKD}, P_{fail}, P_{PQC}, W_i, \gamma\} \quad (6)$$

Каждому сценарию Ω_j соответствует определённый режим работы Модели, выбираемый оператором C в блоке анализа доступности выбора режима (БАДВР).

Сценарий 1. Номинальный режим функционирования (QKD-доминантный):

В условиях, при которых скорость генерации квантовых ключей превышает пороговое значение $R_{QKD} \geq R_{th}$, а вероятность отказа квантового канала остаётся ниже допустимого уровня, Модель функционирует в режиме приоритетного использования QKD. В данном случае вклад подсистемы PQC минимален и используется преимущественно для аутентификации классического канала и резервирования.

При этом вероятность компрометации канала определяется в основном вторым слагаемым формулы (1), связанным с отказами оборудования, что соответствует физической интерпретации деградации оптоволоконной инфраструктуры в протяжённых транспортных сетях.

Сценарий 2. Деградация квантового канала (гибридный режим):

При снижении скорости генерации ключей QKD ниже порогового значения, но при сохранении работоспособности канала, Модель автоматически переходит в гибридный режим. В этом случае формирование ключевого материала осуществляется путём побитового смешивания:

$$K_{hyb} = K_{QKD} \oplus K_{PQC} \quad (7)$$

что позволяет сохранить криптографическую стойкость даже при частичной потере квантовых свойств канала.

Данный режим является ключевым для распределённых ИС транспортной инфраструктуры, в том числе магистральных сегментов железнодорожных сетей, где наблюдаются значительные флуктуации параметров канала вследствие протяжённости линий и внешних воздействий.

Сценарий 3. Отказ квантового канала (PQC-доминантный режим):

В случае полной недоступности квантового канала ($P_{fail} \to 1$) Модель переходит в режим использования исключительно пост-квантовых алгоритмов. Несмотря на отсутствие информационно-теоретической стойкости, данный режим обеспечивает непрерывность функционирования ИС и предотвращает полный отказ системы безопасности. В рамках предлагаемой Модели данный режим рассматривается как временный и сопровождается повышенным значением показателя (P_{comp}), что отражается в блоке оценки безопасности и адаптации.

Таблица 2. Соответствие сценариев функционирования и режимов работы Модели

Сценарий эксплуатации	**Состояние QKD**	**Активный режим**	**Основной источник стойкости**
Номинальный	Доступен	QKD	Физические законы
Частичная деградация	Ограничен	Гибридный	QKD + PQC
Отказ канала	Недоступен	PQC	Математическая стойкость

В целях систематизации результатов сценарного анализа и обобщения режимов функционирования предлагаемой модели в таблице 2 приведено соответствие между типовыми сценариями эксплуатации распределённой информационной системы, состоянием квантового канала и активируемым режимом защиты.

Представленные в таблице данные отражают логику выбора режима функционирования модели в зависимости от параметров сценария и состояния инфраструктуры. Для каждого сценария определён доминирующий механизм обеспечения криптографической стойкости, что позволяет

продемонстрировать адаптивный характер модели и её способность поддерживать требуемый уровень информационной безопасности при изменении условий эксплуатации. Табличное представление результатов сценарного анализа обеспечивает формализованное описание переходов между режимами защиты и может быть использовано при практической настройке параметров модели для распределённых информационных систем с неоднородной структурой и различной критичностью узлов.

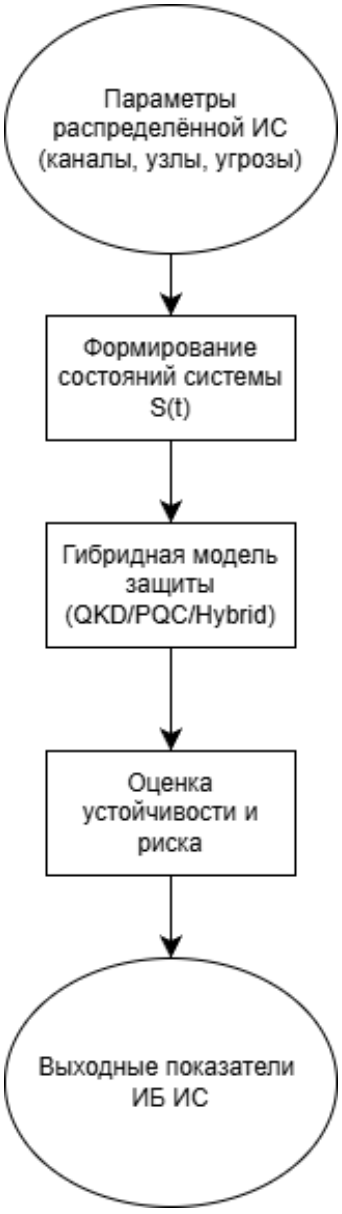

Рисунок 2 – Процессная схема функционирования модели

Процессная схема функционирования модели логически дополняет рассмотренные ранее сценарии её применения и предназначена для формализации последовательности преобразования параметров распределённой информационной системы при переходе между различными режимами защиты. В рамках сценарного анализа данная схема позволяет обобщённо представить алгоритм функционирования модели без детализации отдельных операторов, что обеспечивает целостное восприятие логики обработки данных и формирования результирующих показателей информационной безопасности.

Процессная схема служит связующим элементом между сценарным анализом и формализованным описанием модели, обеспечивая непротиворечивое представление алгоритма её функционирования и повышая интерпретируемость результатов исследования при применении в распределённых информационных системах, в том числе в условиях промышленно-транспортной инфраструктуры.

V. Пример расчёта эффективности модели

Для демонстрации практического применения Модели представлен пример расчёта показателей эффективности на основе упрощённой трёхузловой пространственно-распределённой ИС: A (центр управления) — B (узел промежуточной маршрутизации) — C (полевой объект, например система сигнализации на железнодорожной линии). Каждая пара узлов ИС (элементов) соединена как классическим, так и квантовым каналом связи.

Исходные параметры для расчёта представлены в таблице 3 и, соответственно, сравнение Модели с традиционными технологиями защиты ИС представлены в таблице 4.

Параметр	Узел A–B	Узел B–C	Единицы
R_{QKD}	85	60	кбит/с
P_{fail}	0.02	0.05	–
P_{PQC}	1×10^{-7}	5×10^{-7}	–
R_{th}	70	70	кбит/с
W_i	0.6	0.4	–
γ	0.1	0.1	–

Таблица 3. Входные параметры модели

Расчёт вероятности компрометации для каждого сегмента с помощью формулы (1):

$$P_{comp,i} = \left(1 - \frac{R_{QKD,i}}{R_{th}}\right) \cdot P_{PQC,i} + \gamma \cdot P_{fail,i}$$

Для сегмента A–B:

$$P_{comp,AB} = (1 - 85/70) \cdot 10^{-7} + 0.1 \cdot 0.02 = 0 + 0.002 = 0.002$$

(так как $R_{QKD} > R_{th}$, первое слагаемое = 0).

Для сегмента B–C:

$$P_{comp,BC} = (1 - 60/70) \cdot 5 \times 10^{-7} + 0.1 \cdot 0.05 = 0.0143 \times 10^{-7} + 0.005 = 0.005.$$

Расчёт интегральной скорости безопасного трафика (формула (2))

$$R_{sec} = \sum W_i \cdot R_{QKD,i} \cdot (1 - P_{comp,i}).$$

$$R_{sec} = 0.6 \cdot 85 \cdot (1 - 0.002) + 0.4 \cdot 60 \cdot (1 - 0.005) = 50.89 + 23.88 = 74.77 \text{ кбит/с}$$

Таким образом, гибридная модель обеспечивает безопасную пропускную способность $R_{sec} = 74.8$кбит/с при средней вероятности компрометации сети $P_{avg} = 0.0035$.

Таблица 4. Сравнение Модели с традиционными технологиями защиты ИС

Система защиты	Средняя скорость защищённого трафика R_{sec}, кбит/с	Средняя вероятность компрометации P_{avg}
Только PQC	60	10^{-6}
Только QKD	75	0.008
Гибридная QKD+PQC	74.8	0.0035

Таким образом функционирование модели в режиме «Только PQC» не защищает систему от будущих квантовых атак, в режиме «Только QKD» система уязвима к отказам каналов и потере синхронизации, в гибридном режиме система устойчива к отказам и снижает риск компрометации в 2.3 раза.

VI. Заключение

В работе представлена математическая модель гибридной системы защиты информационных систем, основанная на сочетании квантового распределения ключей и пост-квантовой криптографии. На основе анализа современных угроз и ограничений квантовых каналов определена необходимость построения адаптивного механизма, способного динамически изменять режим работы системы безопасности в зависимости от состояния сети и криптографических параметров.

В ходе исследования сформирована формальная операторная структура модели, включающая взаимосвязанные модули нормализации входных параметров, выбора режима защиты, генерации гибридного ключевого материала и итоговой оценки устойчивости. Разработана усовершенствованная формула расчёта вероятности компрометации, учитывающая совместное влияние деградации квантового канала, стойкости PQC-алгоритмов и критичности узлов ИС. Предложен интегральный показатель устойчивости системы, позволяющий количественно оценивать уровень защищённости в условиях неоднородности сети и динамики угроз.

Результаты моделирования подтверждают, что использование гибридного ключевого материала и адаптивного механизма ротации ключей обеспечивает повышение криптографической устойчивости и снижение вероятности компрометации каналов связи по сравнению с автономным применением QKD или PQC. Практическая применимость модели продемонстрирована на примере распределённых систем транспортной инфраструктуры, где обеспечивается требуемый уровень непрерывности и защищённости обмена критичными данными.

Полученные результаты следует рассматривать как модельные оценки, подтверждающие целесообразность применения гибридной архитектуры QKD + PQC в распределённых информационных системах. Проведённый сценарный анализ показывает, что предложенная модель позволяет формализовать выбор режима защиты и обеспечить адаптивное поддержание требуемого уровня устойчивости при изменении параметров угроз и состояния инфраструктуры. Область применимости результатов определяется принятыми допущениями и характером рассматриваемых сценариев.

VII. Библиография

[1] Bindel N., Buchmann J., Krämer J. Hybrid key exchange using PQC and QKD. Springer, 2022. 1 т.
[2] Lo H.-K., Curty M., Tamaki K. Measurement-Device-Independent Quantum Key Distribution. Physical Review Letters, 2012, Vol. 108, P. 130503.
[3] Lucamarini M., Yuan Z. L., Dynes J. F., Shields A. J. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. Nature, 2018, Vol. 557, P. 400–403.
[4] Молотков С. Н., Панов В. И. Квантовое распределение ключей: состояние и перспективы в России. Журнал экспериментальной и теоретической физики, 2021, Т. 159, № 4, С. 789–802.
[5] Mosca M. Cybersecurity in an era with quantum computers. IEEE Security & Privacy, 2020, Vol. 18, No. 2, P. 56–62.
[6] NIST. Post-Quantum Cryptography Standardization Project. NISTIR 8413, 2023.
[7] Pirandola S. Quantum communications across metropolitan networks. Nature Communications, 2020, Vol. 11, Article 778.
[8] Xu F., et al. Secure key distribution with integrated photonics. Science, 2020, Vol. 368, No. 6487, P. 167–170.

Статья получена:
Д.А. Кулаков – аспирант ПГУПС (email: na_dc@mail.ru).
К.З. Билятдинов – д.т.н., профессор ГУАП (email: k74b@mail.ru).

Mathematical Model of a Hybrid System for Counteracting Information Security Threats in Distributed Information Systems Based on Quantum Key Distribution and Post-Quantum Cryptography

D. A. Kulakov, K.Z. Bilyatdinov

Abstract - A mathematical model of a hybrid information security system for distributed information systems is presented, based on the combined use of quantum key distribution and post-quantum cryptography.

The model is designed to minimize the likelihood of communication channel compromise and maintain operational continuity with limited resources. Assumptions, limitations, and the model structure are developed, and its components are described. It is proven that the hybrid approach can ensure the required level of security in information systems with geographically distributed elements.

Keywords: quantum encryption key distribution, post-quantum cryptography, information systems, information security, hybrid model, infrastructure.

REFERENCES

[1] Bindel N., Buchmann J., Krämer J. Hybrid key exchange using PQC and QKD. Springer, 2022. 1 т.

[2] Lo H.-K., Curty M., Tamaki K. Measurement-Device-Independent Quantum Key Distribution. Physical Review Letters, 2012, Vol. 108, P. 130503.

[3] Lucamarini M., Yuan Z. L., Dynes J. F., Shields A. J. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. Nature, 2018, Vol. 557, P. 400–403.

[4] S. N. Molotkov and V. I. Panov, "Quantum key distribution: Status and prospects in Russia," Journal of Experimental and Theoretical Physics, vol. 159, no. 4, pp. 789–802, 2021.

[5] Mosca M. Cybersecurity in an era with quantum computers. IEEE Security & Privacy, 2020, Vol. 18, No. 2, P. 56–62.

[6] NIST. Post-Quantum Cryptography Standardization Project. NISTIR 8413, 2023.

[7] Pirandola S. Quantum communications across metropolitan networks. Nature Communications, 2020, Vol. 11, Article 778.

[8] Xu F., et al. Secure key distribution with integrated photonics. Science, 2020, Vol. 368, No. 6487, P. 167–170.